
WAMPAC FRAMEWORK - ADMIN MANUAL

The Wide Area Monitoring, Protection and Control (WAMPAC) framework is developed with associated computational algorithms and software tools, to prevent and mitigate cyber-attacks and achieve resilience. The application is designed in accordance with CIA guidelines for information security.

In this network we have a server, set of verifiers and user nodes. Server is the administrator of the network, nodes are desktops who are the participants who take part in transactions, verifiers are set of 7 desktops who are also participating nodes but help in decision making for disputes or root cause analysis in the network.

Every node in the network has a unique decentralized identity (DID). A smart contract governs user enrollment and disenrollment processes based on whitelisted rules.

A distributed Network Monitoring service constantly monitors the entire network for anomalies and performs a PBFT based decision making process on agreed group policies.

The service also detects anomalies, localizes the affected node and provides the latest committed safe state.

A desktop application runs on startup to manage the provenance-monitoring tool.

This admin manual will help through each step of the application. Follow the steps to seamlessly setup the application on the system

Table of Contents

PREFACE	3
Prerequisites	3
Product Elements	3
Admin Server and Verifiers	
SETUP	4
Installation	4
Configuring Syslog Client and Server	4
ADMIN PROCEDURES	7
Whitelist New Nodes	7
Set Rules and Group Policies	8
VERIFIERS PROCEDURES	9
Decentralised Identity Creation	9
Verification	10
Dashboard	11
Log analysis	11
File Sharing	13
Network Monitoring System	16
TROUBLESHOOTING	17
APPENDIX	17

PREFACE

Pre Requisites

1. Java 11
2. Go IPFS v0.6
3. Windows 10 Desktop enterprise edition
4. Network device (Cisco SG300, 28 port Gigabit managed switch)
5. Syslog Servers (Ubuntu 18.04 with rsyslog installed)
6. List of ports mentioned in 5.a are opened

Product Elements

1. **User Interface:** It provides provision for verifiers to generate a unique identity in network, verify identity, file share access permission, continuous monitoring of system status, accessing list of backups of files, and provision to create backups for the logs
2. **Network Identity Creation:** Provision to create a unique decentralized identity (DID) in the network, Verification of the identity is mandatory to perform any operation in the network.
3. **Access Permissions:** Provision to define the file access permissions to specific set of users, Perform operations on the file by checking the permission set , File Versioning – History of the file operations performed
4. **NMS logging module:** Checks Health of system, Periodic log collection and distributed storage of logs, System restoration, Backup logs used for root cause analysis
5. **Active Directory Service:** Admin system who handles the entire network, Enroll users into the network, Setting rules for access policies and group policies, Periodically pushes the system configuration into the network for failover of admin machine (if required)

Admin Server and Verifiers

Our WAMPAC Framework holds two types of Verifiers: Admin Server and Set of Quorum. Admin holds control over the entire. It is charged with user whitelisting, creating and maintaining rules and group policies for the network.

Verifiers are set of nodes who are quorum members part of the Blockchain. They are the members assigned to store provenance data and to perform all the distributed decision making in the network.

SETUP

Installation

- Install all the prerequisites mentioned in Preface.Prerequisites
- Double click on the executable and the UI screen pops up to perform necessary operations

If the executable does not load correctly, please refer troubleshooting section

Configuring Syslog Server and Client

- Configuring a system logging on network device

For any network device which is part of the network, say, Switch or Router, would need to be configured with Syslog client logging configuration.

Please find below configuration of syslog in a SG300 switch through CLI and GUI.

Configuration through CLI:

1. Open the Cisco command-line interface and begin a session
2. Switch to global configuration mode, type the command
 - a. Configure terminal
3. Verify that logging is enabled, if logging is disabled, type the command
 - a. Logging on
4. Configure the switch to send the logs to the syslog server, type the command
 - a. Logging host <ip-address of syslog server> port 514 severity <informational>
5. Return to privileged EXEC mode by typing the command
 - a. End

Configuration through GUI:

1. Login to the cisco GUI and begin a session
2. Go to the system log settings, type the commands mentioned below:
 - a. Administration > System Log > Log Settings.
 - b. In the logging field enable the check box for syslog logging, enable checkbox to enable Syslog Aggregator, set Max. Aggregation time to 300, Under RAM Memory Logging and Flash Memory Logging, check the appropriate check boxes respectively.

Log Settings

Logging: ☒ Enable
 Syslog Aggregator: ☒ Enable
 Max. Aggregation Time: sec. (Range: 15 - 3600, Default: 300)

RAM Memory Logging		Flash Memory Logging	
Emergency:	<input checked="" type="checkbox"/>	Emergency:	<input checked="" type="checkbox"/>
Alert:	<input checked="" type="checkbox"/>	Alert:	<input checked="" type="checkbox"/>
Critical:	<input checked="" type="checkbox"/>	Critical:	<input checked="" type="checkbox"/>
Error:	<input checked="" type="checkbox"/>	Error:	<input checked="" type="checkbox"/>
Warning:	<input checked="" type="checkbox"/>	Warning:	<input type="checkbox"/>
Notice:	<input checked="" type="checkbox"/>	Notice:	<input type="checkbox"/>
Informational:	<input checked="" type="checkbox"/>	Informational:	<input type="checkbox"/>
Debug:	<input type="checkbox"/>	Debug:	<input type="checkbox"/>

c. Click on Apply

3. Go to Remote log Server's setup, type the commands below:

- a. Administration > system log > Remote Log Servers
- b. Click on Add to setup a remote syslog server

Remote Log Servers

Remote Log Server Table					
<input type="checkbox"/>	Log Server	UDP Port	Facility	Description	Minimum Severity
0 results found.					
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>					

- c. Select Server definition as "By IP address", IP Version as "version 4", Under Log Server IP Address input the ip-address of the syslog server, update the port number as "514", facility as "local 3", description as "log" and minimum severity as "informational".

Server Definition: ☒ By IP address ☐ By name
 IP Version: ☐ Version 6 ☒ Version 4
 IPv6 Address Type: ☐ Link Local ☐ Global
 Link Local Interface:
 Log Server IP Address/Name:
 UDP Port: (Range: 1 - 65535, Default: 514)
 Facility:
 Description:
 Minimum Severity:

- d. Click on Apply

Remote Log Servers					
Remote Log Server Table					
<input checked="" type="checkbox"/>	Log Server	UDP Port	Facility	Description	Minimum Severity
<input checked="" type="checkbox"/>	192.168.1.20	514	Local 3	Test log	Warning
<div>Add... Edit... Delete</div>					

- Configuration on Ubuntu Syslog Server
 1. The default logging utility in Ubuntu is Rsyslog. Login to the Ubuntu machine and open Terminal. In the terminal go to the file rsyslog.conf:
 - a. `cd /etc/`
 - b. `gnome-open rsyslog.conf`
 2. The below line should be present in the file, rsyslog.conf. Type the command below:
 - a. `$IncludeConfig /etc/rsyslog.d/*.conf`
 3. Make a new file, *cisco.conf* in */etc/rsyslog.d* directory.
 - a. `cd /etc/rsyslog.d`
 - b. `cat cisco.conf`
 4. Add the content below to the file *cisco.conf* to make sure all syslog messages with facility local7 should be logged to the *cisco.log* file at the directory */var/log/cisco*.
 - a. `Local7.*`
 - b. `/var/log/cisco/cisco.log`
 5. Create a folder named *cisco* at */var/log* and a file *cisco.log* inside that folder.
 - a. `mkdir /var/log`
 - b. `cat cisco.log`
 6. Restart rsyslog daemon, type the command below:
 - a. `sudo service rsyslog restart`

NOTE: Since windows machines do not have rsyslog, we have to go with Ubuntu syslogs to log system information and events of the switch. All logs sent from the switch should be available now at the location */var/log/cisco/cisco.log*.

ADMIN PROCEDURES

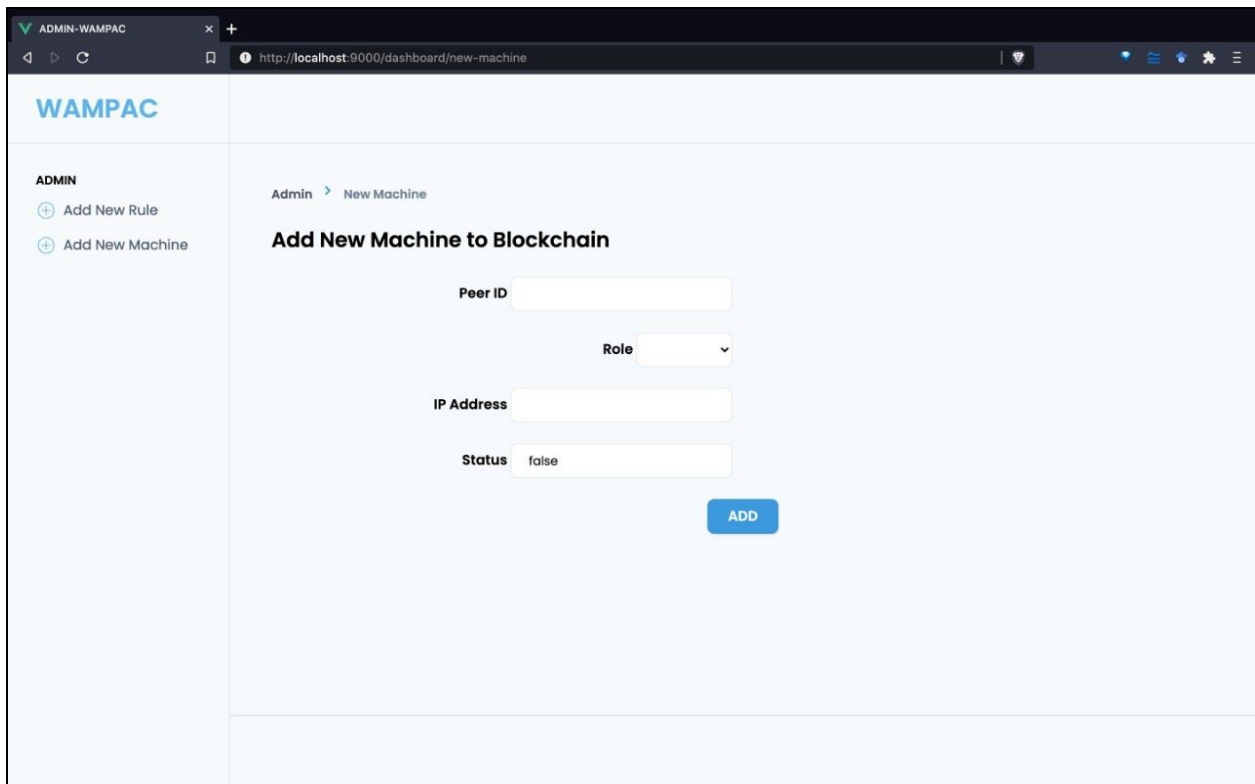
This section explains how to use the product categorized based on the operations provided for the Admin Server

Whitelisting New Nodes

A smart contract governs user enrollment and disenrollment processes based on whitelisted rules.

The server node whitelists nodes based on IP Address and defines role (user or verifier). The whitelist node information is shared to all the verifier nodes.

1. Enter the PeerID of the new user, the IP address and the role
2. Click ADD to add the new user



The screenshot shows a web browser window with the URL `http://localhost:9000/dashboard/new-machine`. The page title is "WAMPAC". On the left, there is a sidebar with the "ADMIN" section containing two links: "Add New Rule" and "Add New Machine". The main content area is titled "Admin > New Machine" and "Add New Machine to Blockchain". It contains a form with the following fields: "Peer ID" (text input), "Role" (dropdown menu), "IP Address" (text input), and "Status" (text input with the value "false"). A blue "ADD" button is located at the bottom right of the form.

Setting Rules and Group Policies

The screenshot shows the WAMPAC Admin interface in a web browser. The browser's address bar displays `http://localhost:9000/dashboard/new-rule`. The WAMPAC logo is in the top left corner. A sidebar on the left contains the 'ADMIN' section with two links: 'Add New Rule' and 'Add New Machine'. The main content area is titled 'Admin > New Rule' and 'Add New Rule to Blockchain'. It contains several input fields: 'Admin Machine' (a text field), 'Start Date' (a date-time field with a placeholder 'hh:mm:ss A'), 'End Date' (a date-time field with a placeholder 'hh:mm:ss A'), 'Error Threshold' (a text field), 'Login Threshold' (a text field), 'Warning Threshold' (a text field), and 'Other Threshold' (a text field). A blue 'ADD' button is positioned below the 'End Date' field.

1. Enter the following fields

Admin Machine: Hostname of the admin machine

Start Date: Date from which the rule is applicable to the network

End Date: Date at which the rule expires

Error Threshold: Threshold each system can commit errors

Login Threshold: Total number of times each system can make an invalid login before an action is taken

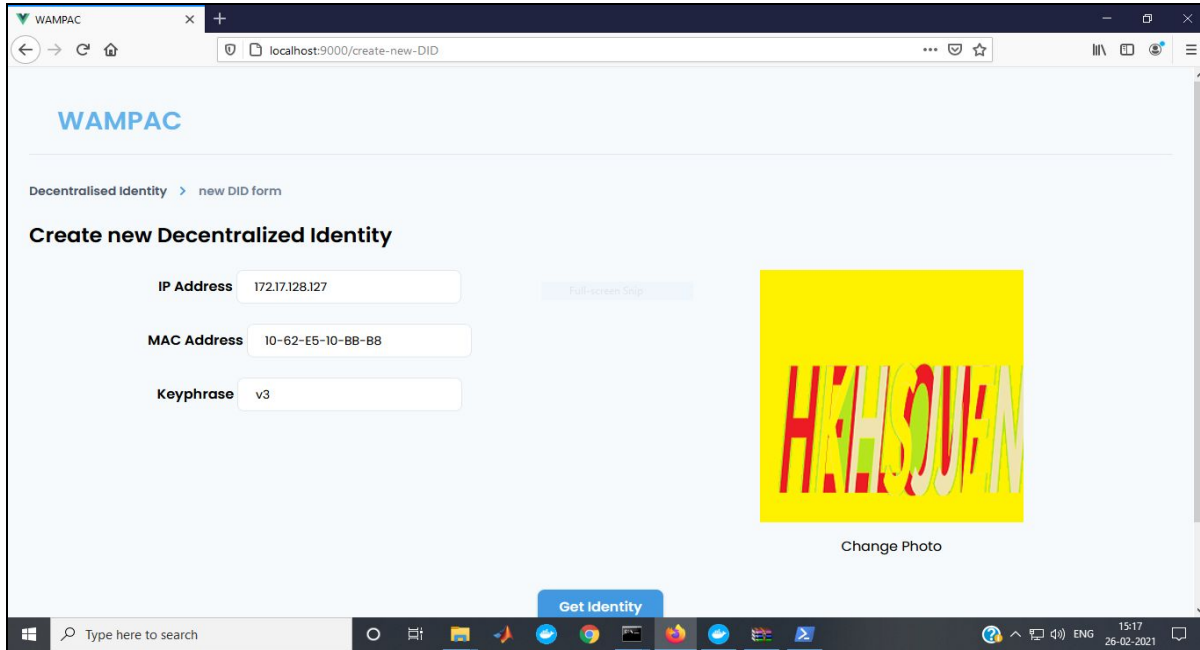
Warning Threshold: Total number of warnings each system is given before an action is taken

Other Threshold: Total number of times each system can make anomalies before an action is taken

2. Click ADD

VERIFIERS PROCEDURES

Decentralised Identity Creation



The screenshot shows a web browser window with the address bar displaying 'localhost:9000/create-new-DID'. The page title is 'WAMPAC'. Below the title, there is a breadcrumb trail 'Decentralised Identity > new DID form'. The main heading is 'Create new Decentralized Identity'. The form contains three input fields: 'IP Address' with the value '172.17.128.127', 'MAC Address' with the value '10-62-E5-10-B8-B8', and 'Keyphrase' with the value 'v3'. To the right of these fields is a 'Full-screen Snap' button. Below the input fields is a 'Get Identity' button. To the right of the 'Get Identity' button is a yellow square placeholder for a profile picture with the text 'CHANGE PHOTO' below it. The browser's taskbar is visible at the bottom, showing various application icons and the system clock indicating 15:17 on 26-02-2021.

The above screen will be displayed on successful running of the application. Follow the below steps to create and identity

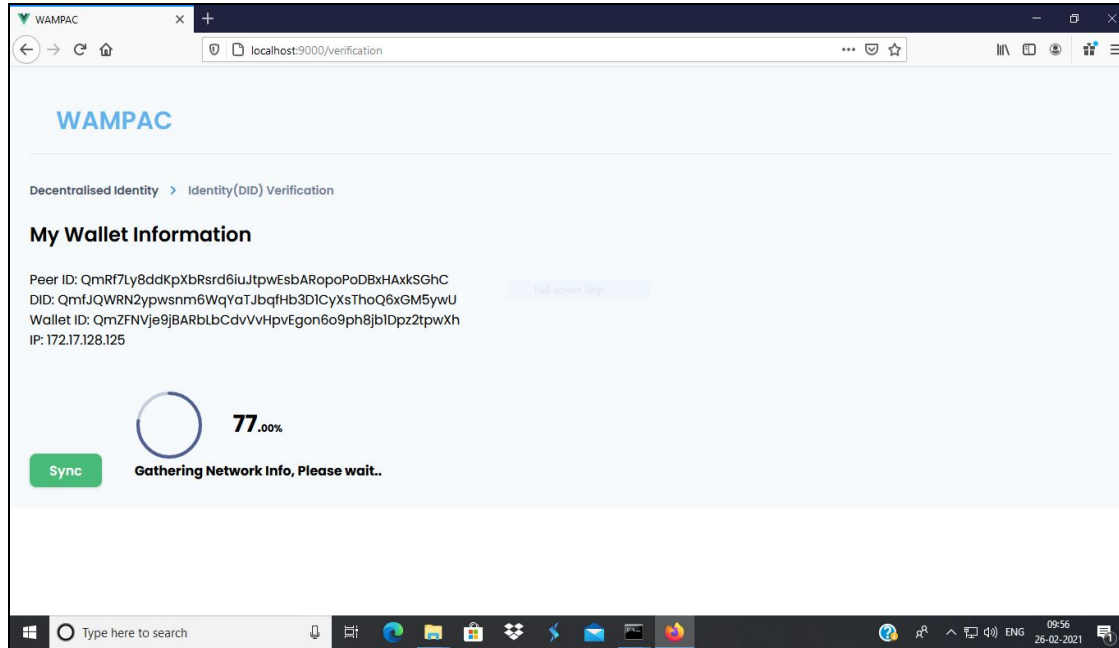
Steps

1. Type in the Key Phrase (random Seed) - supports any character type
2. IP and Mac address fields are automatically detected
3. Drag and drop and image of size 256 * 256, format *PNG
4. Click on Get Identity to obtain a unique network id.

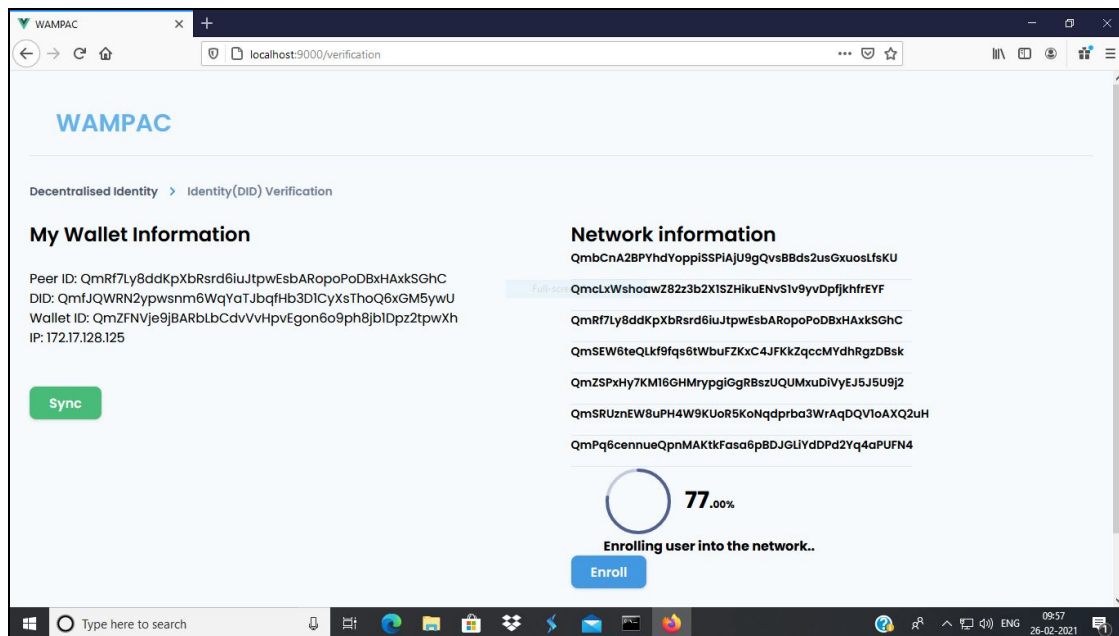
Note: All the input fields are mandatory

On successful identity creation, the page redirects to the Verification page. If failure, **retry**

Verification



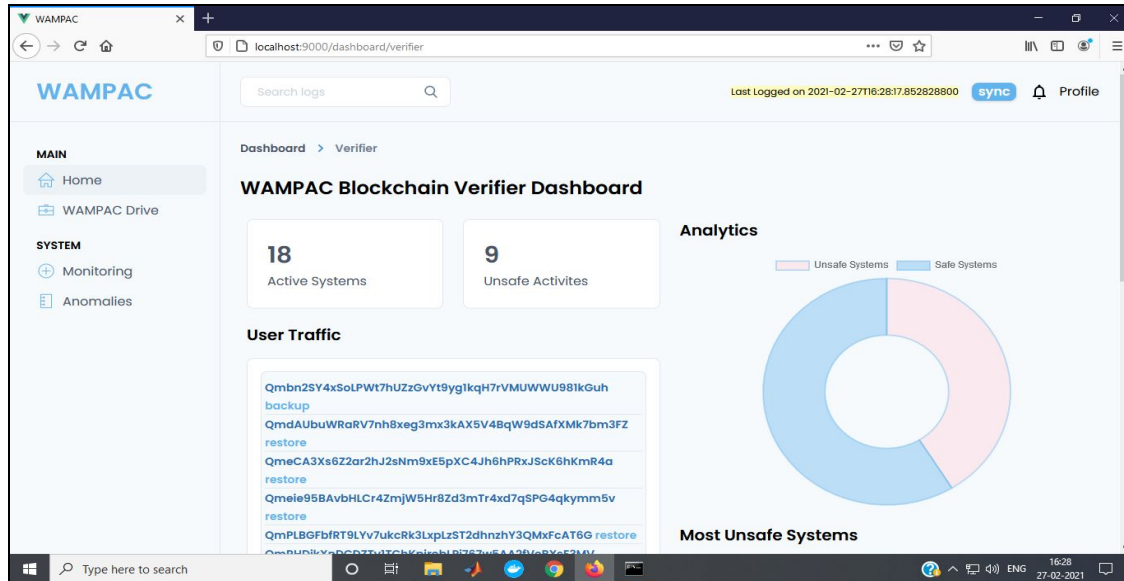
This page displays the wallet information of the verifier. Click on Sync, to obtain the network information



Once the network information is synchronized, click on Enroll, to get your identity verified. If Verified, page redirects to home page & you are authorized to perform any operation in the network based on your role. If not, you are not allowed to join the network.

Dashboard

After successful Identity creation and enrollment into the network, the application will be redirected to the main dashboard with a set of operations made available

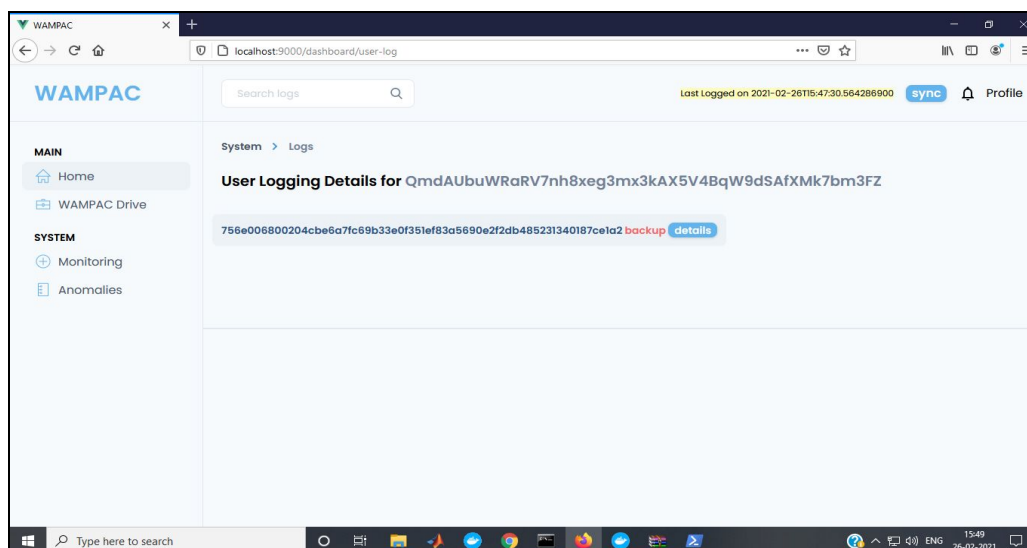


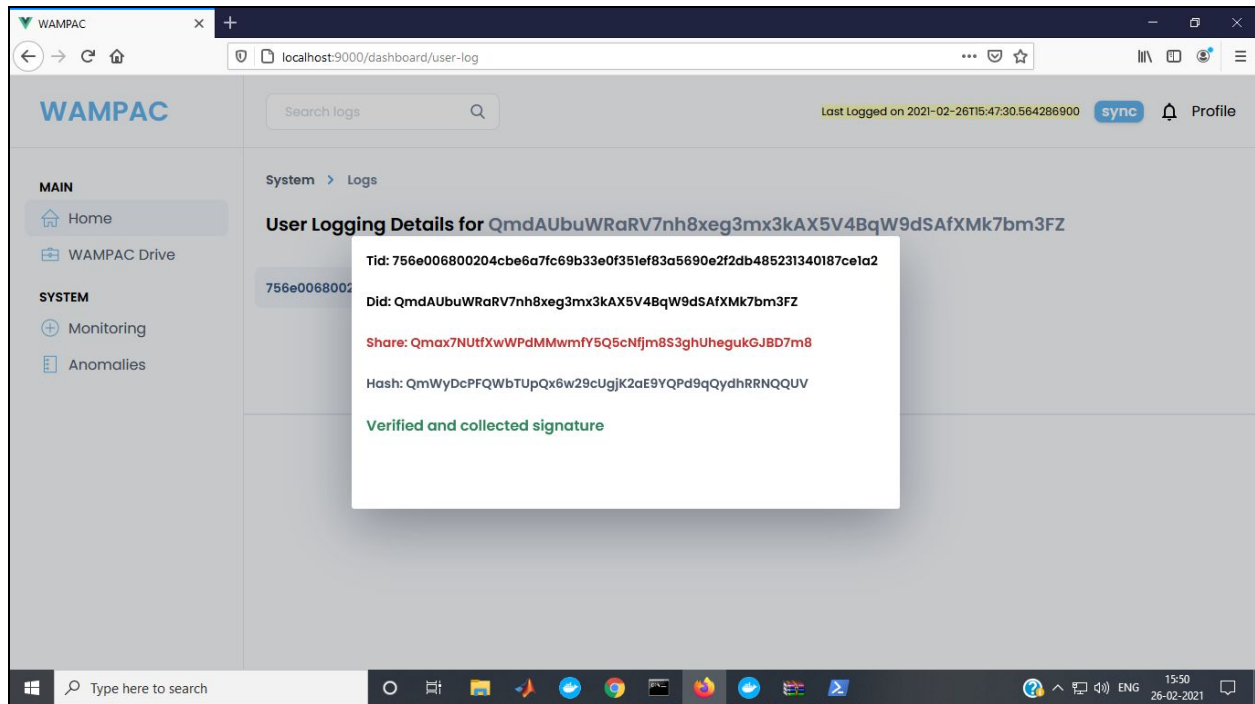
On dashboard verifiers can visually overview the following about the whole network

1. Total number of nodes active in the network
2. Number of anomalies committed by different nodes
3. Log collection

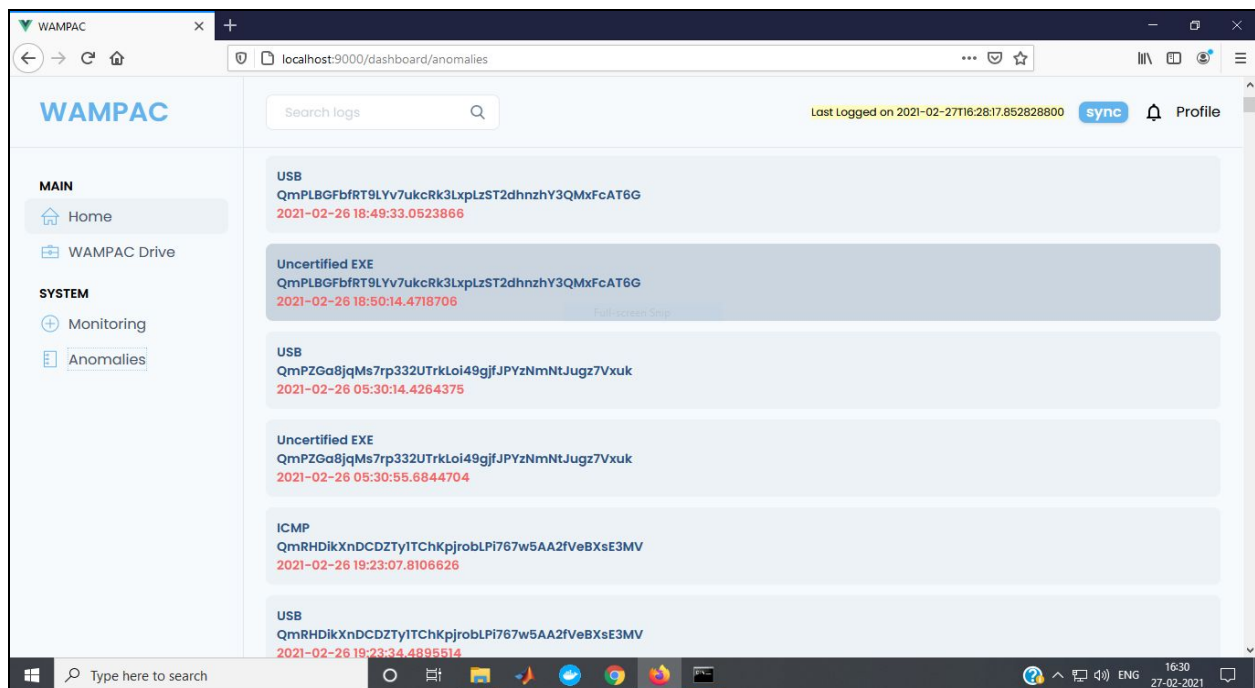
Log Analysis

Verifiers can view and track the transactions committed by user nodes to the network regarding the NMS logs and anomaly reports



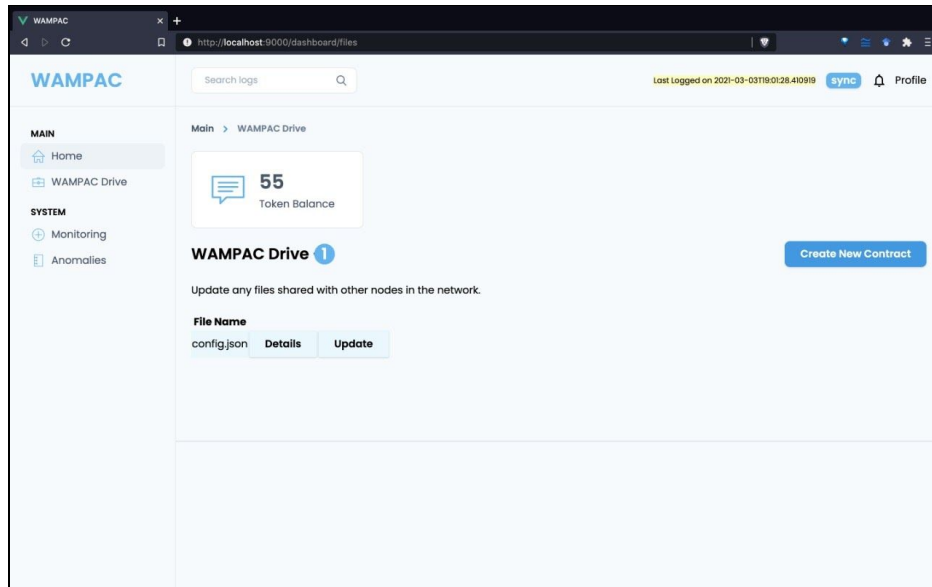


The history of anomalies committed by the user nodes and its corresponding details like time, type of anomaly, decision after reporting to the network can be tracked



File Sharing - WAMPAC Drive

In this page, you can view the list of shared files and its details. In order to create a new shared file and set permission levels, click on Create New Contract

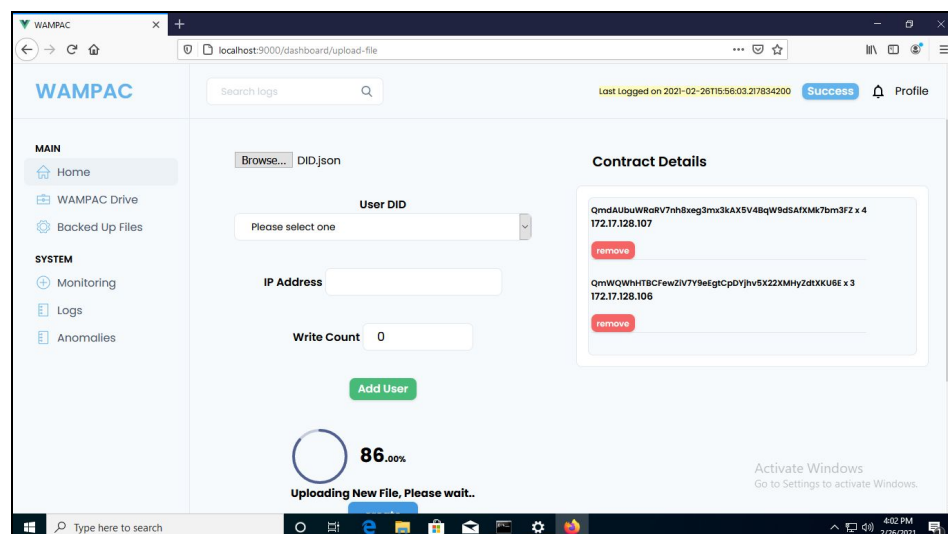


A. Create Contract

Follow the steps to create a new shared file

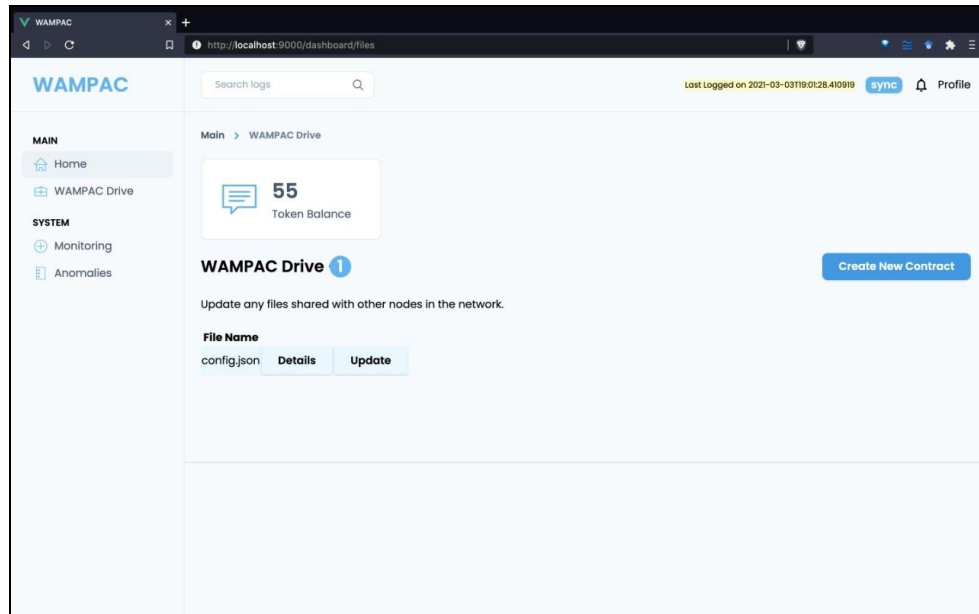
Steps

1. Import a file you want to share
2. Click the drop-down button to choose the identity of user who should access the contract
3. IP address of the corresponding user is auto filled
4. Type in the number of times that particular user has access
5. Click on add user button to add the access level details to the contract

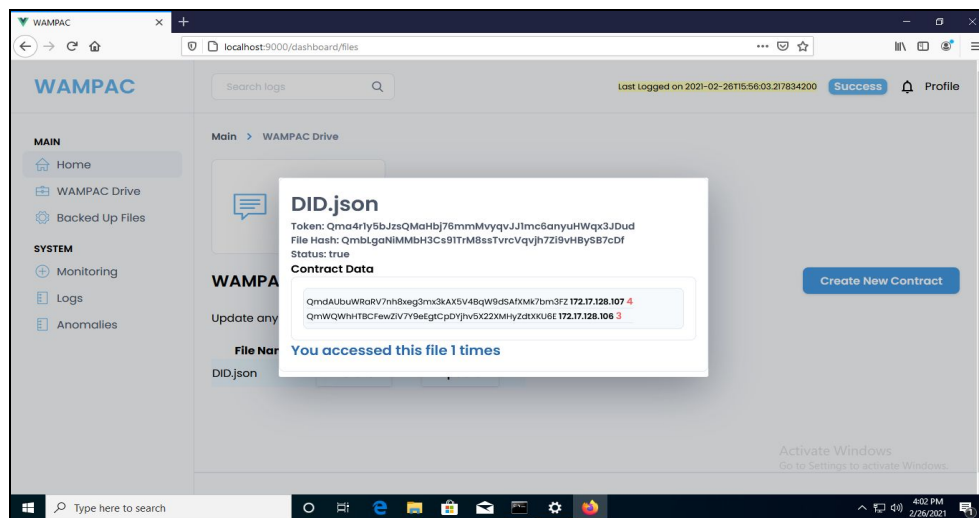


Note: Add your own identity to the contract since you are the initiator of the file sharing process - Mandatory

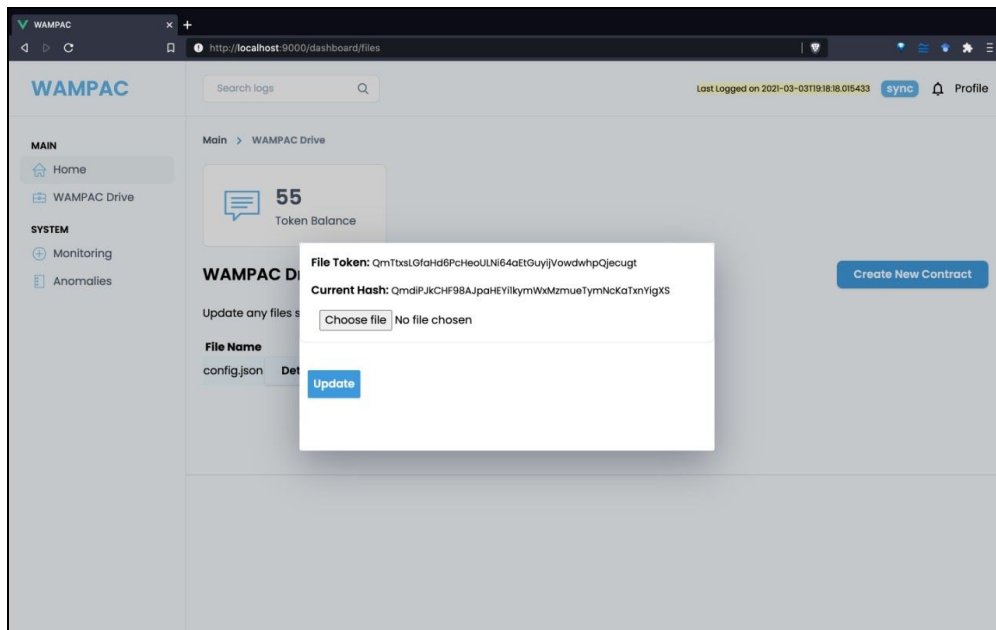
6. After adding the required members, click on create to initiate the file sharing process
7. After successful file sharing process, you will see the shared file details as below



8. Click on Details to view more information about the shared file



B. File Operation - Update

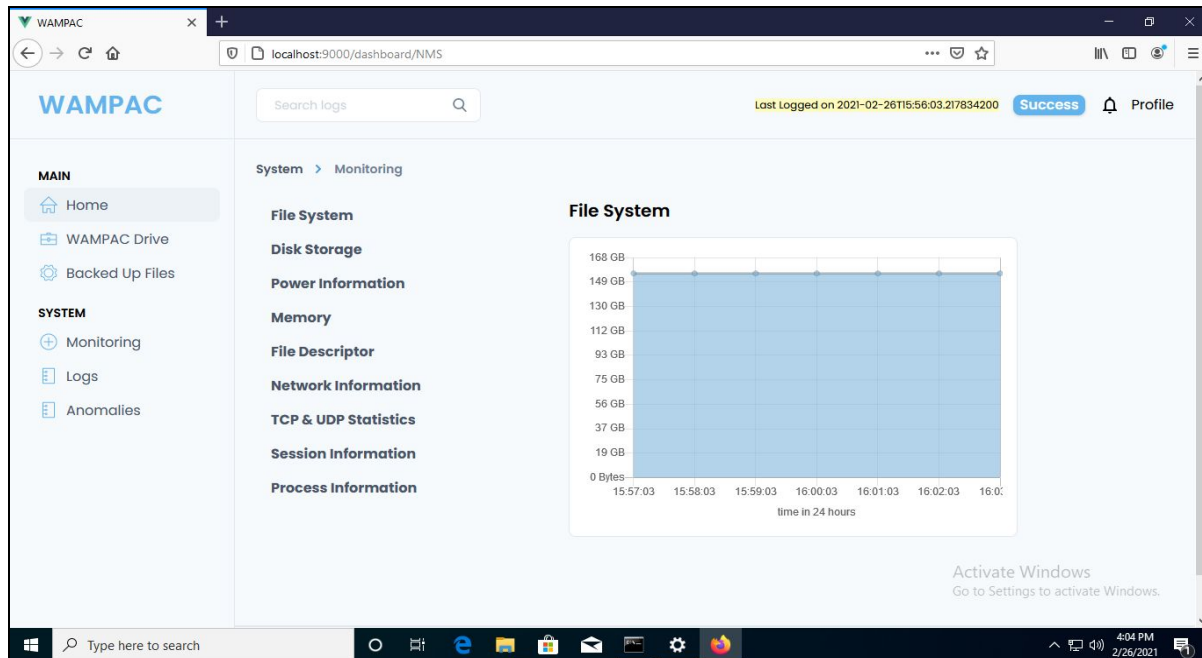


In order to update a particular file, Click on update button next to the file

The current version details of the file are displayed. Select the next version of the file you want to update and click on update

The access permissions set in the creation stage is verified among the specified set of identities while updating the new version of the file

Network Monitoring System



A web UI by default on startup should run the provenance-monitoring tool listening for an incoming message.

In the Monitoring screen there are four graphs namely Memory, Disk Storage, File System and File Descriptor continuously running in the background collecting respective data every one minute to help populate the graphs.

Other components like Power Information, Network Information, TCP and UDP Statistics, Session Information, Process Information generate relevant information where their respective buttons are clicked.

TROUBLESHOOTING

1. Executable not loading while installation
 - Go to “Task Manager” and check if required prerequisites are running
 - If not, kill executable from the task manager and re-run the exe
2. UI does not load
 - Check if the port is open – contact network admin (refer Appendix for port details)
3. UI Stuck
 - Go to Task Manager and kill all the running services related to the product (ipfs, java & exe)

APPENDIX

List of Ports

IPFS – 4001,5001,8080

Electron – 9000

Jar – 1898

Internal communication – 15010, 15011, 15040, 8787